## ABSTRACT

The inventive methods and systems provide an approach to protecting unencrypted sensitive information from being paged out to secondary storage, such as a hard disk, during paging operations. In the described embodiment, a key is provided and is maintained in the main memory of a virtual memory system. Measures are taken to protect the key such as page-locking the key in the main memory to ensure that it never gets paged out to the secondary storage. The described key is a desirably large key that is randomly generated by the operating system. When sensitive information is to be placed in the main memory, it is encrypted with the page-locked key. The encrypted sensitive information can then be paged out to secondary storage without concern about its security. When the encrypted sensitive information is needed by a process or application, it is retrieved from secondary storage and decrypted using the page-locked key. For further protection, the sensitive information can be decrypted into a page-locked page of main memory. More than one key can be used to encrypt and/or decrypt the sensitive information.